Z-Wave Factsheet

fbinna, vmeier, laquino 2016

Generell

Einsatzgebiet	Home-Automation
Topologie	Mesh
Range	bis zu 100m zwischen 2 Nodes
Maximaler Range	Durchschnittlich 200m (Weiterleitung über 4 Hops)
Anzahl Geräte pro Netzwerk	232

Gerätetypen

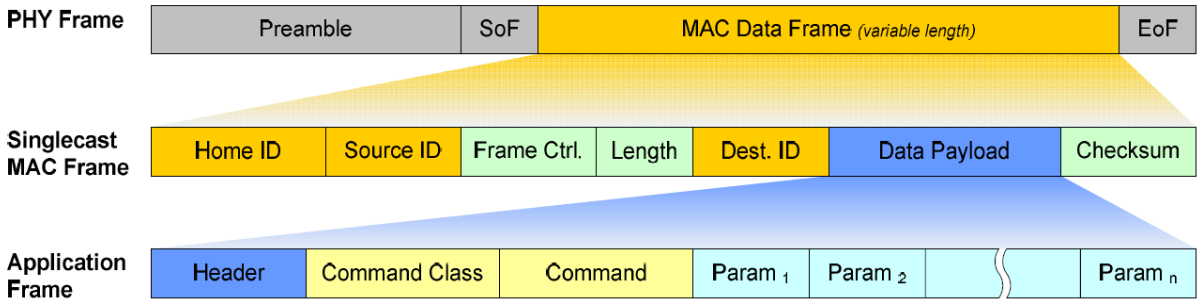
- Elektrische Schalter (ergänzend oder Ersatz für physischen Schalter)
- Elektrische Dimmer (ergänzend oder Ersatz für physischen Schalter)
- Motoren (zum Öffnen / Schliessen von Fenstern, Rollläden etc.)
- Bildschirme, LED-Displays, Sirenen etc. (Signal-Quellen)
- Sensoren (Themometer, Hygrometer etc.)
- Thermostat Controller (Thermostat Radiator Valves, Bodenheizung-Controller etc.)
- Fernbedienungen (Universelle Infrarot-Fernbedienungen, spezielle Z-Wave Fernbedienungen ...)
- USB Sticks und IP Gateways (für Fernsteuerung über PC / über Internet)

Netzwerk-Informationen

Ein Netzwerk besteht jeweils aus einem (oder in Spezialfällen aus mehreren) Controller und mehreren Slaves. Die Komponenten können über eine HomeID und NodeID eindeutig identifiziert werden.

HomeID	32bit; Hersteller weist dem Controller eine ID zu, der die HomeID des Netzwerks bestimmt
NodeID	8bit; Controller weist allen Slaves eine NodeID zu

Protokoll-Spezifikationen



Physical Layer

Datenübertragungs-rate	9.6kbps / 40kbps / 100kbps
Frequenz	**Europa**: 868.42 MHz (SRD); **USA**: 908.42 MHz (ISM)
Encoding	Machester (9.6kbps) / NRZ (40kbps / 100kbps)
Maximaler Range	Durchschnittlich 200m (Weiterleitung über 4 Hops)
Anzahl Geräte pro Netzwerk	232

Transport Layer

Zuständig für Retransmission, Packet acknowledgement, Packet origin authentication und Node-Wakeups. Auf dieser Schicht werden folgende Informationen übermittelt:

Information	Grösse	Funktion
HomeID	32bit	Identifikation des Netzwerks
Source NodeID	8bit	NodeID der Quelle
Frame-Typ	8bit	Gibt an, ob es sich um Singlecast, Multicast oder Broadcast handelt
Control Flag	?	Flag für Lowpower etc.
Payload length	8bit	Länge der Payload
Destination NodeID	8bit	NodeID des Ziels
Authentication Header	8 Byte	Origin Authentication Header, falls in Secure Transmission Mode
Checksumme	8bit	Checksumme des Frames (für Integritätschecks)

Netzwork Layer

Unter anderem zuständig für Netzwerk-Discovery und Routing. Geräte die direkt an eine Stromquelle angeschlossen sind, können als Packet-Repeater dienen (keine batteriebetriebenen Geräte).

Application Layer

Parst die Frame-Payload und entschlüsselt die enthaltenen Informationen mit dem Shared-Secret.

Command classes

Z-Wave kommuniziert den Geräten, unabhängig von deren Funktionalität, Kommandos über 3 verschiedene "Command classes". Die Interpretation des übertragenen Kommandos ist dann den Geräten überlassen.

Name	Wertrange	Funktion
SET	0 - 255	Setzen eines Wertes
GET	-	Anfrage des aktuell eingestellten Wertes
REPORT	0-255	Response mit aktuellem Wert auf GET-Request

Security

Key-Exchange

Das Bestimmen eines Shared-Keys von Controller und Node findet während des intialen Pairing statt und läuft wie folgt ab:

1. Controller generiert Encryption Key K_n für Key-Exchange (Pro Netzwerk einmal generiert)
2. Controller verschlüsselt K_n mit einem temporären default Key (hardcoded, aus Firmware)
3. Übertragung an Node
4. Node entschlüsselt K_n mit default Key aus Firmware

Mit dem erhaltenen Schlüssel werden zwei weitere Keys, der Frame-Encryption-Key K_c und der Data-Origin-Authentication-Key K_m, ausgemacht:

$$K_c = AES - ECB_{K_n}(Password_c)$$
$$K_m = AES - ECB_{K_n}(Password_m)$$

$Password_c$ und $Passwort_m$ sind fest in der Firmware hinterlegte Werte.

Übersicht:

Preshared Encryption Key K_n	128bit; Von Controller bei Netwerk-Setup generiert
Frame-Encryption-Key K_c	128bit; Wird im AES-OFB-Algorithmus zur Verschlüsselung eines Frames verwendet
Data-Origin-Authentication-Key K_m	128bit; Key für das Frame-Hashing mit AES-CBCMAC
Nonce	64bit; Gegen Replay-Attacken

Eignung im Bereich IoT

Energieverbrauch

Die Z-Wave Technologie versucht den Energieverbrauch möglichst gering zu halten. Das wird erreicht, indem die Z-Wave Units im power-safe Modus arbeiten und so nur 0.1% aktiv sind. Durch den geringen Energieverbrauch können die Z-Wave Units in batteriebetriebenen Geräten (z.B. Fernbedienungen, Rauchmelder und Sensoren) verbaut werden.

Eignungsbereiche

SmartHome

Z-Wave arbeitet im sub-gigahertz Bereich, und vermeidet so die Überlagerung mit Wifi- und Bluetoothtechnologien. Bei der Entwicklung wurde speziell beachtet, dass die Reichweite, durch Wände und andere Hindernisse nicht zu stark beeinträchtigt wird.

Outdoor

Z-Wave wurde ursprünglich für den Gebrauch in Gebäuden entwickelt. Es ist aber prinzipiell Möglich auch Systeme im Freien zu entwickeln. Die Reichweite beträgt ungefähr 100m (Die SAW filter des Herstellers Sigma Design begrenzen die Richweite auf 30m), das heisst es ist mit Hilfe eines Netzes möglich grössere Flächen abzudecken.

Entwicklung

Für die Entwicklung ist kein teures SDK nötig. Es gibt eine freie API (open-zwave), die es ermöglicht auf verschiedensten Systemen Z-Wave Technologie einzusetzen. Zudem ist ein Raspberry PI "daughter board" verfügbar, die den Einsatz solcher Chips nochmals vereinfacht.

Kostenpunkt

Die Z-Wave Geräte sind nicht günstig, weil vieles in fertigen Geräten, wie Glühbirnen, Schaltern und anderen Home-Devices, schon integriert ist.

Gerät	Preis (CHF)
Controller	100-300
Module(Dimmer/Thermostat)	50-100
Sensoren	50-100
Zwischenstecker	20-75
Fernbedienungen	50
Kameras	300-400
Glühbirne	70-80
Sirenen/Alarm	80

Quellen

Offizielles Z-Wave FAQ
BlackHat 2013 - Hacking Z-Wave
Z-Wave Europe Wiki - Handbook (Linksammlung)
Z-Wave Europe Wiki - Application Layer Details
Wikipedia - Z-Wave Z-Wave Security Evaluation